



Document Summary



New
Search



Help

[Preview Claims](#)

[Preview Full Text](#)

[Preview Full Image](#)

Email Link: 

Document ID: JP 2000-089666 A2

Title: ENCODING/DECODING DEVICE

Assignee: NIPPON TELEGR & TELEPH CORP

Inventor: SUGITA MAKOTO

US Class:

Int'l Class: G09C 1/00 A; H04L 9/06 B

Issue Date: 03/31/2000

Filing Date: 09/16/1998

Abstract:

PROBLEM TO BE SOLVED: To achieve an encoding/decoding device capable of ensuring guarantee of higher safety than a conventional one.

SOLUTION: In an encoding/decoding device which encodes and decodes data at every block of a constant bit length by plural steps of encoding processing using a common secret key to the decoding and encoding, an encoding function part for realizing an encoding function is configured of non-linear processing parts 301-1-301-4 executing the disturbing calculations by using a common key created from a secret key for an inputted data and outputting the calculation results, and linear processing parts 302-1-302-3 inputting the data outputted from the non-linear processing parts and executing predetermined linear calculations and outputting the calculation results, with the 4 steps of the non-linear processing parts and the 3 steps of the linear processing parts alternately cascaded.

(C)2000,JPO

THIS PAGE BLANK (USPTO)

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号
特開2000-89666
(P2000-89666A)

(43)公開日 平成12年3月31日(2000.3.31)

(51)Int.Cl. ⁷	識別記号	F I	テーマコード(参考)
G 0 9 C 1/00	6 1 0	G 0 9 C 1/00	6 1 0 A 5 J 1 0 4
H 0 4 L 9/06		H 0 4 L 9/00	6 1 1 A

審査請求 未請求 請求項の数1 O L (全 7 頁)

(21)出願番号 特願平10-262073

(22)出願日 平成10年9月16日(1998.9.16)

(71)出願人 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(72)発明者 杉田 誠

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(74)代理人 100064908

弁理士 志賀 正武

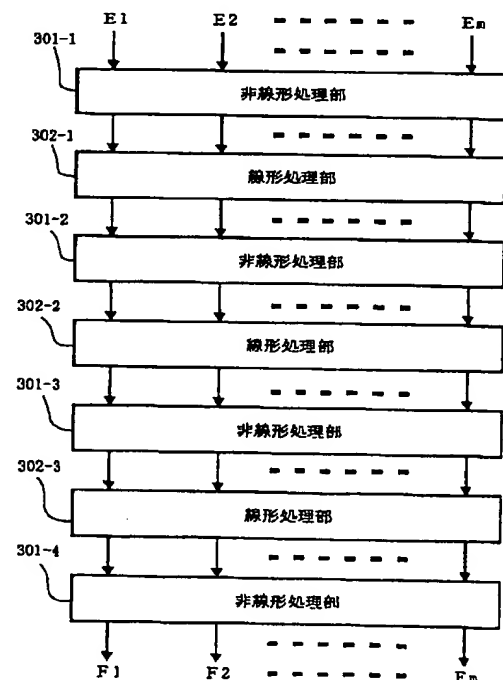
Fターム(参考) 5J104 AA01 JA10 NA08

(54)【発明の名称】 暗号化／復号化装置

(57)【要約】

【課題】従来に比べより高い安全性の保証が可能な暗号化／復号化装置を実現する。

【解決手段】復号化および暗号化に共通の秘密鍵を用い、複数段の暗号化処理段によって、一定のビット長のブロック毎にデータの暗号化および復号化を行う暗号化／復号化装置において、複数段の暗号化処理段において暗号化関数を実現する暗号化関数部が、入力されたデータに対して秘密鍵から生成された鍵を用いて攪乱演算を行って演算結果を出力する非線形処理部301-1～301-4と、非線形処理部から出力されたデータを入力し、所定の線形演算を行って演算結果を出力する線形処理部302-1～302-3とを、交互に、非線形処理部を4段と、線形処理部を3段、縦段接続して構成されている。



【特許請求の範囲】

【請求項1】 復号化および暗号化に共通の秘密鍵を用い、一定のビット長のブロック毎にデータの暗号化および復号化を行う暗号化／復号化装置において、各段の入力データの半分のビット数を有する第1のデータを所定の暗号化処理を行う暗号化関数部に入力して得られる該暗号化関数部の出力を入力データの他の半分のビット数を有する第2のデータにビット毎にXORして得られる第3のデータと、第1のデータとを出力する暗号化処理段を、互いに複数段接続し、該複数段の暗号化処理段によって暗号化／復号化処理を複数回繰り返し行うことでデータの暗号化又は復号化を行うものであって、

前記暗号化関数部が、

入力されたデータに対して秘密鍵から生成された鍵を用いて攪乱演算を行って演算結果を出力する非線形処理部と、

非線形処理部から出力されたデータを入力し、所定の線形演算を行って演算結果を出力する線形処理部とを、交互に、非線形処理部を4段と、線形処理部を3段、縦段接続してなることを特徴とする暗号化／復号化装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明は共通鍵暗号アルゴリズムにおけるブロック暗号方式を用いた暗号化／復号化装置に係り、特に、差分解読法や線形解読法に対して強い暗号化／復号化装置に関する。

【0002】

【従来の技術】 図1に、暗号化および復号化において共通の秘密鍵を用いる共通鍵暗号の一方式であるデータの暗号化および復号化を一定のまとまった長さ毎に行うブロック暗号方式による暗号化および復号化装置（以下、暗号化／復号化装置）の基本的な機能構成を示す。図1に示す暗号化／復号化装置は、 j 個のそれぞれ暗号化／復号化処理を行う暗号化処理段 $101-1, 101-2, \dots, 101-j$ から構成されている。この暗号化／復号化装置は、64ビット、128ビット等の一定のブロック長毎に平文 S 又は暗号文 T を入力して、複数の暗号化処理段 $101-1, 101-2, \dots, 101-j$ によって暗号化又は復号化処理を複数回繰り返し行い、それぞれ入力文と同一のブロック長を有する暗号文 U 又は平文 V を出力する。各暗号化処理段 $101-1, 101-2, \dots, 101-j$ では暗号化／復号化処理の際に、秘密鍵のデータに基づく計算処理が行われる。その際、各暗号化処理段 $101-1, 101-2, \dots, 101-j$ では、1つの複数ビットの秘密鍵からビット単位の転置、シフト等により生成された異なる複数の鍵が使用される。なお、暗号化と復号化の処理では、各暗号化処理段 $101-1, 101-2, \dots, 101-j$ で用いられる複数の鍵の使用順序が互いに逆順となる。また、以下

の説明では暗号化と復号化で共通する事項に対して、暗号化に関連する名称、用語を代表して使用する。

【0003】 図2は、図1における暗号化処理段 $101-1 \sim 101-j$ の各段における機能構成を示すブロック図である。図2に示す暗号化処理段は、2つの入力に対してビット毎に排他的論理和を行って出力する排他的論理和回路（以下、XOR回路） $201-i$ と、複数ビットからなる鍵を用いた暗号化処理を行う暗号化関数部 $202-i$ から構成されている。入力 S 、あるいは前段から出力されたデータのブロック長の左半分のビットの P_{i-1} は、XOR回路 $201-i$ へと入力され、暗号化関数部 $202-i$ の出力 R_i とビット毎に排他的論理和（以下、XOR）が行われて、後段の右半分の入力となる出力 $Q_i (= P_{i-1} (+) R_i)$ として出力される（ $(+)$ はXORを示す）。一方、各段の入力データの右半分のビットの Q_{i-1} は、暗号化関数部 $202-i$ へ入力されるとともに、後段の左半分の入力となる出力 $P_i (= Q_{i-1})$ として出力される。ここで i は図1の暗号化処理段の段数に対応する $1 \sim j$ の整数であり、 P_0 および Q_0 は入力データ S 又は T に、 P_{j+1} および Q_{j+1} は出力データ U 又は V に対応するデータである。

【0004】 図2に示す暗号化関数部 $202-i$ の従来の構成の一例を図7に示す。図7は、共通鍵暗号として広く使用されている「DES暗号」（Data Encryption Standard; 米国NIST (National Institute of Standards and Technology) の規格）（以下、従来技術1と称する）における暗号化関数部の構成を示すブロック図である。図7に示す暗号化関数部 $202-i$ では、入力された32ビットの Q_{i-1} が拡大転置部 801 で所定の転置表（変換表）を用いた拡大転置によって48ビットのデータに変換されてXOR回路 802 へと入力される。XOR回路 802 は64ビットの秘密鍵からあらかじめ生成されていた i 段用の48ビットの鍵と拡大転置部 801 の出力とでXORを行って48ビットのデータを出力する。XOR回路 802 の出力は各6ビットずつに分けられ、8個のSボックスと呼ばれるデータ置換部（ $S1 \sim S8$ ） $803-1 \sim 803-8$ へと入力される。各Sボックス $803-1 \sim 803-8$ では、入力された各6ビットのデータに対して所定の置換表に基づくデータの置き換えが行われて各4ビットのデータが出力される。さらに転置部 804 で所定の転置表に基づいてビット位置の転置が行われて32ビットの処理結果 R_i が求められる。

【0005】 なお、「DES暗号」では、図1に示す暗号化／復号化装置の暗号化／復号化の処理は16回の繰り返しである。また、暗号化／復号化装置の全体の構成としては、図1の構成に対して、入力段と出力段に、それぞれ初期転置処理と逆初期転置処理を行うブロックが追加されている。また、各暗号化処理段では、1つの6

3

4 ビットの秘密鍵から生成されたそれぞれ異なる 16 個の 48 ビットの鍵が使用されるようになっている。

【0006】図 8 に、図 2 に示す暗号化関数部 202-i の他の従来の構成例を示す。図 8 は、NTT（日本電信電話株式会社）によって開発された 128 ビットブロックアルゴリズムを採用した「E2」という共通鍵暗号アルゴリズム（以下、従来技術 2 と称する）における暗号化関数部の構成を示すブロック図である。図 8 に示す暗号化関数部 202-i では、入力された 64 ビットのデータ Q_{i-1} が各 8 ビットのデータ x_1, x_2, \dots, x_8 に分割された後、非線形処理部 901 へ入力される。非線形処理部 901 では、入力されたデータ x_1, x_2, \dots, x_8 が、8 個の XOR 回路によって 128 ビットの秘密鍵から生成された第 1 の鍵 $K(1)$ と XOR されて、その演算の結果が 8 個の S ボックスへそれぞれ入力される。8 個の S ボックスでは、予め定められた置換表を参照することで入力データに対して置換処理が行われ、各 8 ビットのデータ z_1, z_2, \dots, z_8 が出力される。ここで、非線形処理部 901 では、S ボックスというデータ置換部において置換処理を行うことで、出力として、入力データに対して非線形な変換処理を行ったデータが得られることになる。

【0007】非線形処理部 901 から出力されたデータ z_1, z_2, \dots, z_8 に対しては、データ変換層 902 において下式で示す線形演算処理が行われる。

【数 1】

$$\begin{pmatrix} z'_1 \\ z'_2 \\ z'_3 \\ z'_4 \\ z'_5 \\ z'_6 \\ z'_7 \\ z'_8 \end{pmatrix} = P \begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \\ z_5 \\ z_6 \\ z_7 \\ z_8 \end{pmatrix}$$

ここで行列 P は

$$P = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

【0008】なお、図 8 に示すデータ変換層 902 は、16 個の XOR 回路から構成されているが、これは上式を実現する一例であって、内部の構成については限定されない。

【0009】データ変換層 902 から出力された各 8 ビットのデータ z'_1, z'_2, \dots, z'_8 は、非線形処理部 903 へ入力される。非線形処理部 903 では、非線形処理部 901 と同様にして、8 個の XOR 回路を用いて入力データ z'_1, z'_2, \dots, z'_8 と秘密鍵から生成された第 2 の鍵 $K(2)$ とで XOR を行い、さらに 8 個の S ボックスで予め定めた置換表を参照することで置換処理を行い、処理結果として各 8 ビットのデータ y_1, y_2, \dots, y_8 を出力する。

【0010】非線形処理部 903 から出力された各 8 ビットのデータ y_1, y_2, \dots, y_8 には、さらに 8 ビットを単位とする左回転処理が行われる。そして回転処理の結果が暗号化関数の処理結果 R_i として出力される。

【0011】なお、アルゴリズム「E2」では、図 1 に示す暗号化／復号化装置が 12 段の暗号化／復号化処理段を有して構成されている。暗号化／復号化装置の全体の構成としては、図 1 の構成に対して、入力段と出力段に、それぞれ初期変換処理と最終変換処理を行うブロックが追加されている。また、各暗号化処理段では 1 つの

128ビットまたは192ビットもしくは256ビットの秘密鍵から生成されたそれぞれ異なる12個の鍵が使用され、初期変換処理と最終変換処理の各ブロックでは各2個の異なる鍵が使用されるようになっている。

【0012】以上の説明したように、従来技術1においては、図7に示すように各暗号化関数部においてSボックスを用いる非線形な処理を行うデータ置換部が1段設けられ、さらにこの暗号化関数部を有する暗号化処理段を複数段設けることによって安全性の向上が図られている。従来技術2では、図8に示すように暗号化関数において、Sボックスを用いる非線形処理部で置換されたデータを線形処理部で変換し、さらに、もう一度Sボックスを用いる非線形処理部でデータを置換することにより、さらなる安全性の向上を図っている。

【0013】

【発明が解決しようとする課題】しかしながら上記従来の装置は、最大平均差分確率という暗号化の強度評価（最悪値が1、最良値が p^{-27} 、 p は0以上1以下の値）として最も一般的な尺度において、従来技術1の場合で1、従来技術2の場合で p^{12} であり、何れの場合もこの尺度における理論的最大値である p^{-27} に比べて低い安全性しか保証できないという課題があった。

【0014】この発明の目的は、従来技術に比べより高い安全性の保証が可能な暗号化／復号化装置を実現することにある。

【0015】

【課題を解決するための手段】上記課題を解決するため、請求項1記載の発明は、復号化および暗号化に共通の秘密鍵を用い、一定のビット長のブロック毎にデータの暗号化および復号化を行う暗号化／復号化装置において、各段の入力データの半分のビット数を有する第1のデータを所定の暗号化処理を行う暗号化関数部に入力して得られる該暗号化関数部の出力を入力データの他の半分のビット数を有する第2のデータにビット毎にXORして得られる第3のデータと、第1のデータとを出力する暗号化処理段を、互いに複数段接続し、該複数段の暗号化処理段によって暗号化／復号化処理を複数回繰り返すことによりデータの暗号化又は復号化を行うものであって、前記暗号化関数部が、入力されたデータに対して秘密鍵から生成された鍵を用いて攪乱演算を行って演算結果を出力する非線形処理部と、非線形処理部から出力されたデータを入力し、所定の線形演算を行って演算結果を出力する線形処理部とを、交互に、非線形処理部を4段と、線形処理部を3段、縦段接続してなることを特徴としている。

【0016】この発明によれば暗号化／復号化装置の何れにおいても、暗号化関数部において非線形処理部と線形処理部が交互にそれぞれ4段、3段多段縦段接続された暗号化関数を用いることにより、暗号化関数の最大平均差分確率を小さくすることによって全体としての安全

性を高めることができる。

【0017】

【発明の実施の形態】以下、図1～図6を参照して本発明の実施形態について説明する。本発明による暗号化／復号化装置全体としての基本的な構成は、従来の例として説明した「DES」や「E2」のような他のブロック暗号化方式による構成と同様に、図1に示す構造を有している。すなわち本発明による暗号化／復号化装置は、図1に示すように暗号化処理段101-1～101-jが10多段縦段接続された構成を有している。図1では、その多段縦段の初段のデータとして各bビットのブロック長を有する平文S又は暗号文Tが入力され、終段の出力として各bビットのブロック長を有する暗号文U又は平文Vが出力される。

【0018】次に、図1における各暗号化処理段101-1～101-jとしては、従来の技術と同様に図2に示すような構成を用いることができる。各暗号化処理段101-i（iは1～j）には、図2に示すようにブロック長（bビット）をそれぞれ半分に分割したデータ P_{i-1} とデータ Q_{i-1} を入力し、データ Q_{i-1} を暗号化関数部202-iに入力して得られる出力 R_i を、XOR回路201-iによってデータ P_{i-1} にビット毎（bit-wise）のXORして得られる $P_{i-1} (+) R_i$ （（+）はXORを表す）を次段の入力 Q_i とする。また、 Q_{i-1} をそのまま次段の入力 P_i として出力するような構成を考える。

【0019】次に、本発明が特徴とする構成である図2に示す暗号化関数部202-iの構成について説明する。本発明においては、暗号化関数部202-iを、図3に示すように、非線形処理部301-1，301-2，301-3，および301-4と線形処理部302-1，302-2，および302-3が交互にそれぞれ4段と、3段縦段接続された構成とする。非線形処理部301-1，301-2，301-3，および301-4と、線形処理部302-1，302-2，および302-3では、それぞれ入力された平文S又は暗号文Tのブロック長bビットの半分のビットをm分割した値（mは2以上、bの半分以下の整数）と等しいビット数（nビットとする）を有するm個のデータが並列に入出力される。図3では、入力段となる非線形処理部301-1の入力データを E_1, E_2, \dots, E_m 、出力段となる非線形処理部301-4の出力データを F_1, F_2, \dots, F_m としている。

【0020】図3に示す各非線形処理部301-1～301-4は、それぞれ図4に示すように各nビットのデータ $C_1, C_2, C_3, \dots, C_m$ と、各kビットの鍵 K_1, K_2, \dots, K_m とを入力して置換演算を用いた攪乱演算を行って各nビットのデータ $D_1, D_2, D_3, \dots, D_m$ を出力するm個の演算部401-1～401-mから構成されている。これらm個の演算部401-1

7

～401-mは、並列して動作する。各kビットの鍵K₁, K₂, …, K_mは、従来の場合と同様にして1つの秘密鍵から置換、ビットシフト等の処理によって予め生成しておく。なお、非線形処理部において用いる鍵K₁, K₂, …, K_mは、図1の各暗号化処理段101-1～101-j毎に異なる値とすることが望ましい。また、各暗号化処理段内で、あるいは各非線形処理部内で、鍵K₁, K₂, …, K_mを同一の値にすることも可能である。

【0021】図5は、図4に示す非線形処理部の内部構成のより具体的な構成を示すブロック図である。図5に示す非線形処理部は、各nビットの入力C₁, C₂, …, C_mをそれぞれ入力して、入力データと同じビット長の各nビットの鍵K₁, K₂, …, K_mとビット毎のXORをとるXOR回路501-1, 501-2, …, 501-mと、各XOR回路501-1, 501-2, …, 501-mの出力に対して、所定の置換表による置換処理を行うことでデータに対して攪乱演算を行う置換部502-1, 502-2, …, 502-mから構成されている。置換部502-1, 502-2, …, 502-mは、図7～図8を参照して説明した従来の構成におけるSボックスと同様の構成を用いることができる。置換部502-1, 502-2, …, 502-mからは、それぞれnビットのデータD₁, D₂, …, D_mが出力されて、後続する線形処理部へと入力されるか、または最最終段であれば暗号化関数部の出力となる。

【0022】図6に図3に示す線形処理部302-1～302-3の具体的な構成を示す。図6においては行列Aの値を例えば下式のように予め定め、各線形処理部302-1～302-3の入力となる各nビットのデータG₁, G₂, …, G_mに線形作用させる線形変換を定めている。図6に示す構成では、入力データG₁～G_mと、行列Aから、各nビットの出力H₁, H₂, …, H_mを下式のようにして求める。ただし、下式は、平文S又は暗号化文Tのブロック長を128ビット、ブロックの分割数mを8、各データG₁, G₂, …, G_mおよびH₁, H₂, …, H_mのビット数を8ビットとする場合の例である。

【数2】

$$\begin{pmatrix} H_1 \\ H_2 \\ H_3 \\ \vdots \\ H_m \end{pmatrix} = A \begin{pmatrix} G_1 \\ G_2 \\ G_3 \\ \vdots \\ G_m \end{pmatrix}$$

ここで行列Aは

$$A = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

【0023】なお、本発明による暗号化／復号化装置は、論理回路によるハードウェアによって実現することもできるし、計算機とその計算機で実行される暗号化／復号化プログラムとの組み合わせによって実現することも可能である。また、暗号化／復号化プログラムは、計算機読み取り可能な記録媒体に記録して、あるいはネットワークを介して頒布することが可能である。

【0024】

【実施例】上記発明の実施の形態において最大平均差分確率という安全性評価尺度においてj=8の場合に実際に計算することにより各置換の最大平均差分確率をpと定めたとき、暗号化関数部が2^{p8}という理論的最良値(p⁸)に近い値を示し、暗号全体として8^{p24}という高い安全性が保証可能であることが確認された。これは従来技術1、2の場合と比べて高い安全性が保証可能であることを示している。

【0025】

【発明の効果】本発明によれば、4段の非線形処理部と3段の線形処理部を交互に接続してなる暗号化関数部を用いて暗号化処理手段を構成することによって、従来技術に比べ非常に高い安全性の保証が可能な暗号化／復号化装置を実現することが可能になる。

【図面の簡単な説明】

【図1】 ブロック暗号化方式による暗号化／復号化装置の機能構成を示すブロック図である。

【図2】 図1における暗号化処理段の機能構成を示すブロック図である。

【図3】 本発明が特徴とする図2における暗号化関数部の機能構成を示すブロック図である。

【図4】 図3における非線形処理部の機能構成を示すブロック図である。

【図5】 図4における非線形処理部の具体的な構成を示すブロック図である。

【図6】 図3における線形処理部の具体的な構成を示す*

*ブロック図である。

【図7】 従来技術1における暗号化関数部の機能構成を示すブロック図である。

【図8】 従来技術2における暗号化関数部の機能構成を示すブロック図である。

【符号の説明】

101-1～101-j 暗号化処理段

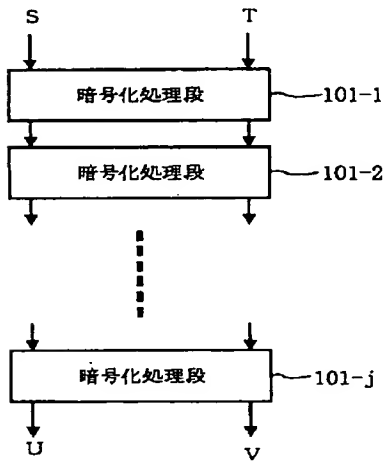
201-i XOR回路

202-i 暗号化関数部

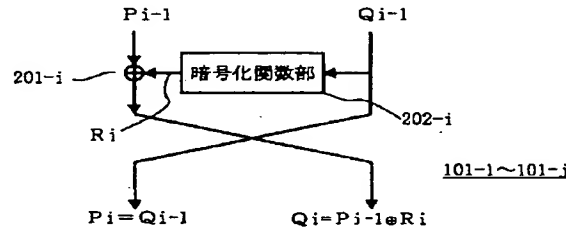
301-1～301-4 非線形処理部

302-1～302-3 線形処理部

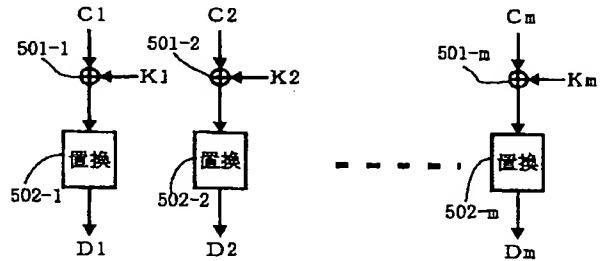
【図1】



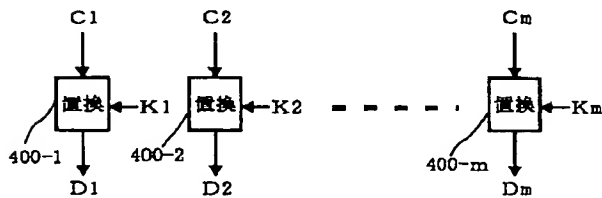
【図2】



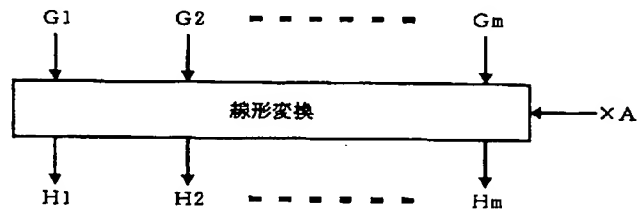
【図5】



【図4】

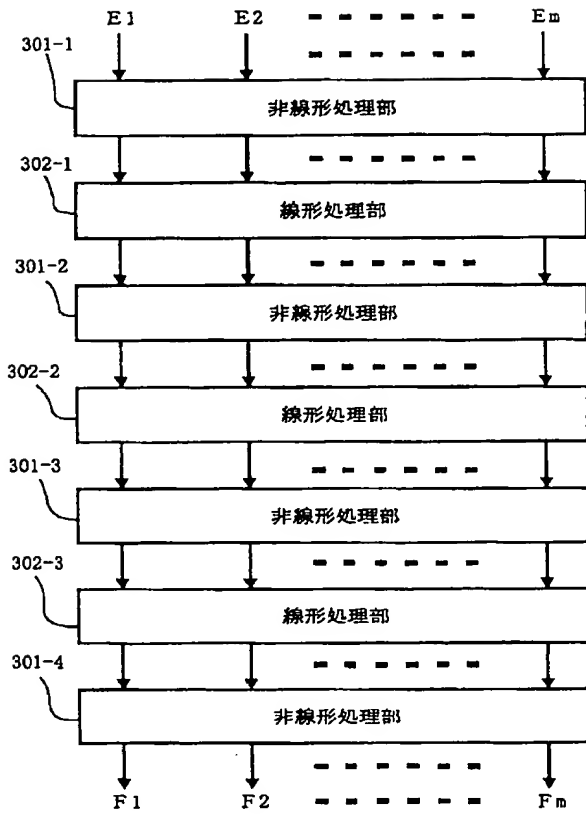


【図6】

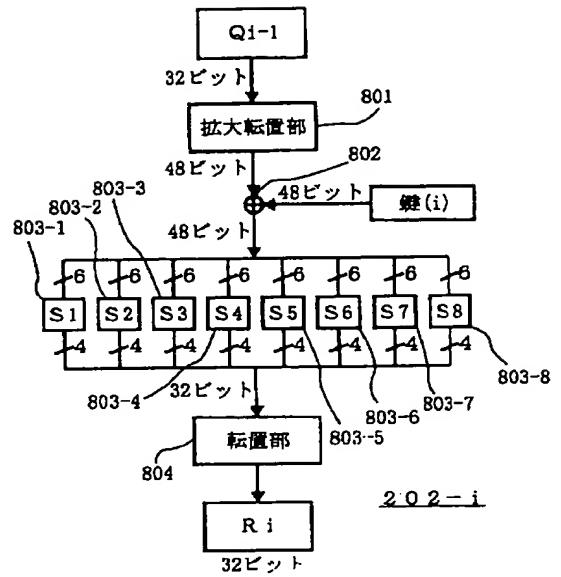


$$A = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

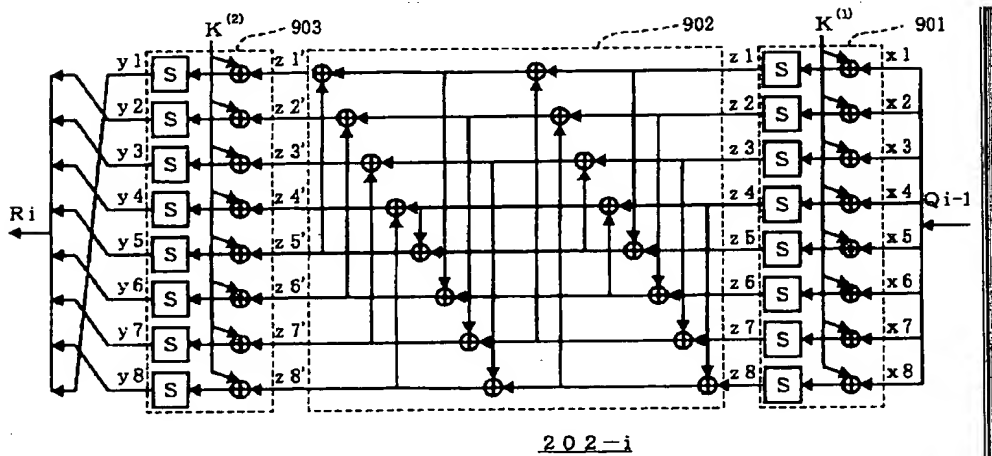
【図 3】



【図 7】



【図 8】



THIS PAGE BLANK (USPTO)